Research Paper | Science | E-ISSN No : 2454-9916 | Volume : 9 | Issue : 10 | October 2023

RANSOMWARE LANDSCAPE: THREATS AND PREVENTION STRATEGIES

Krutiksha Chaudhari[1], Neha Pingle[2]

[1,2] Department of Research and PG studies in Science & Management, Vidyabharti Mahavidyalaya, Camp Road, Amravati

ABSTRACT

Security has been a significant concern for an extended period of time. The emergence of viruses, malware, and ransomware has further compounded the challenges faced by practitioners. This paper aims to explore the threats and prevention of ransomware, and the general characteristics of several popular ransomware variants. In the section on evolution, the paper presents a comprehensive study tracing the development of ransomware from its inception to the present day. This study sheds light on the various types of infections caused by ransomware, including data and machine infections. Different attackers have made targeted choices for their attacks, and the paper provides insights into the various types of targets that ransomware focuses on. To illustrate the severity of the problem, this paper also presents case studies of ransomware attacks. Furthermore, the paper discusses the necessary steps that victims should take after an infection occurs. The researcher also delves into the measures individuals can take to safeguard their systems and prevent ransomware attacks. Finally, the paper concludes by outlining a few recommended steps to protect systems and data.

KEYWORDS: Ransomware, Security, Attack, Cryptowall, Crytolock, Nvidia

1. INTRODUCTION

Malware attacks have become increasingly prevalent in today's digital landscape, with ransomware emerging as one of the most popular and damaging forms of malware. Ransomware operates by infiltrating a person's computer system and encrypting their data, effectively rendering it inaccessible until a ransom is paid to the attacker. While this form of cyber extortion has been around and impact have escalated in recent years.

In 2016, ransomware attacks made headlines as they targeted various industries, including the healthcare sector. These attacks not only disrupted critical services but also compromised sensitive patient data, posing significant risks to individual's privacy and well-being. The healthcare industry, in particular, became a prime target due to its reliance on digital systems and the potential for attackers to exploit vulnerabilities in outdated or poorly secured infrastructure.

Nvidia, the leading global semiconductor chip company, experienced a significant breach as a result of a ransomware attack in February 2022. The company officially acknowledged that the threat actor responsible for the attack had initiated the unauthorized disclosure of employee credentials and proprietary information on the internet.

The ransomware group, known as Lapsus$, claimed responsibility for the attack and asserted that they had obtained and were prepared to release 1 terabyte of company data. In addition to this, Lapsus$ demanded a payment of $1 million form Nvidia, as well as a percentage of an unspecified fee.

Numerous media reports initially indicated that Nvidia had to temporarily suspend certain aspects of its operations for a period of two days due to the compromise of its internal systems. However, the company later refuted these claims, asserting that the attack had not adversely affected its business activities in any manner.

In response to the ransomware attack, Nvidia promptly implemented enhanced security measures and promptly engaged the services of cyber incident response experts to mitigate the situation. Some sources even suggest that Nvidia may have retaliated against the hackers by infiltrating their systems and deploying ransomware. However, the veracity of these claims remains unverified and uncorroborated.

To mitigated the risks associated with ransomware attacks, experts consistently advise individuals and organizations to regularly back up their data. By maintaining secure and up-to-date backups, victims can restore their systems without having to succumb to the attacker's demands. However, despite this advice, many individuals still opt to pay the ransom due to various reasons. Some may lack the technical knowledge or resources to restore their systems independently, while others may fear the potential consequences of not complying with the attacker's demands.

The rise of ransomware attacks underscores the urgent need for improved cybersecurity measures and increased awareness among individuals and organizations. It is crucial to invest in robust security solutions, regularly update software, and educate users about the risks and preventive measures associated with malware attacks. By staying vigilant and implementing proactive measures, individuals and organizations can better protect themselves against the growing threat of ransomware and other forms of malware.

Furthermore, ransomware attacks are becoming more sophisticated and targeted, with attackers using social engineering tactics to trick users unto downloading and installing malware. They may also use advanced encryption techniques to make it more difficult for victims to recover their data without paying the ransom. Additionally, ransomware attacks are increasingly being carried out by organized criminal groups, who have the resources and expertise to develop and

deploy highly effective attacks.

This article concludes that ransomware, in many respects, benefits from traditional malware development techniques. However, there are distinct characteristics of ransomware that offer advantages to defenders. At a fundamental level, the objective of ransomware often involves a reversible denial-of-service(DoS) attack on data availability. In practical terms, this entails performing cryptographic operations on user data modifying numerous data files. Defenders can leverage these features to enhance both the detection of and protection against ransomware in ways that are not applicable to malware in general.

2. HISTORY OF RANSOMWARE ATTACKS:

The history of ransomware attacks can be traced back to 1989 when the "AIDS virus" was utilized to extort funds from ransomware recipients. The payment for this attack was sent to Panama, and a decryption key was subsequently sent back to the user. In 1996, Moti Yung and Adam Young from Columbia University introduced ransomware known as "cryptoviral extortion", which was born out of academic research. This concept illustrated the progression, strength, and creation of modern cryptographic tools. The first cryptovirology attack was presented at the 1996 IEEE Security and Privacy Conference, where the virus contained the attacker's public key and encrypted the victim's files. The malware then prompted the victim to send asymmetric ciphertext to the attacker to decipher and return the decryption key for a fee.

Over the years, attackers have become increasingly creative by requiring payments that are nearly impossible to trace, which helps cybercriminals remain anonymous. For instance, the notorious mobile ransomware Fusob requires victims to pay using Apple iTunes gift cards instead of standard currencies like dollars. The popularity of ransomware attacks has soared with the growth of cryptocurrencies such as Bitcoin, which is a digital currency that uses encryption techniques to verify and secure transactions and control the creation of new units. Attackers prompt victims to use other popular victims to use other popular cryptocurrencies such as Ethereum, Litecoin, and Ripple.

Ransomware attacks have targeted organizations in nearly every vertical, with one of the most famous viruses being the attacks on Presbyterian Memorial Hospital. This attack infected labs, pharmacies, and emergency rooms, highlighting the potential damage and risks of ransomware. Social engineering attackers have become more innovative over time, as evidenced by a situation where new ransomware victims were asked to have two other users install the link and pay a ransom to decrypt their files, as reported by the Guardian.

3. TYPES OF RANSOMWARES:

1. Scareware
2. Encrypting ransomware
3. Screen lockers
4. Mobile ransomware
5. Doxware
6. DDoS extortion
7. Ransomware-as-a-Service(RaaS)

3.1 Scareware:

It is one of the common types of ransomwares, which deceives users by presenting a false warning message claiming that malware has been detected on the victim's computer. These attacks often masquerade as antivirus solutions and demand payment to remove the non-existent malware.

3.2 Encrypting ransomware:

It is also known as crypto-ransomware, is another prevalent form of ransomware. It encrypts the victim's files and demands payment in exchange for a decryption key.

3.3 Screen lockers:

It is designed to restrict the victim's access to their computer, preventing them from accessing any files or data. Typically, a message is displayed that demands payment in order to unlock the computer.

3.4 Mobile ransomware:

Mobile ransomware specifically targets devices such as smartphones and tablets. It demands payment in order to unlock the device or decrypt the data stored on it.

3.5 Doxware:

It is a sophisticated type of ransomware that poses a significant threat. It threatens to publish sensitive, explicit, or confidential information from the victim's computer unless a ransom.

3.6 DDoS extortion:

It is a form of ransomware that involves threatening to launch a Distributed Denial of Service(DDoS) attack against the victim's website or network unless a ransom payment is made.

3.7 Ransomware-as-a-Service(RaaS):

In this type of ransomware cybercriminals offer ransomware programs to other hackers or cyber-attackers who utilize these programs to target victims.

It is important to note that these are just a few examples of the most common types of ransomwares. As cybercriminals adapt to cybersecurity strategies, they continuously develop new and innovative methods to exploit vulnerabilities and breach computer systems.

4. RANSOMWARE PREVENTION TECHNIQUES:

With the rise of ransomware attacks and the potential economic losses they can cause, individuals are actively seeking ways to prevent such attacks. Over half of reported malware attacks in 2017 were ransomware incidents, highlighting the seriousness of this cyber-crime(Alam et al., 2020). To address this concern, researchers are developing prevention methods and sharing them through research papers. However, only a few methods have proven effective. This section explores previous research on prevention techniques in two main areas: user behavior and system-based approaches.

4.1 User Behavior

User behavior plays a significant role in the susceptibility to ransomware attacks. Careless actions, such as sharing software or application accounts with other and setting weak passwords, can expose vulnerabilities that attackers can exploit to gain unauthorized access to systems. In particular, sharing accounts increases the likelihood of an attacker hacking into the system through compromised credentials. If employees are not vigilant about the security of their logged-in accounts while using organizational devices, attackers may take advantage of this and launch ransomware attacks to hold data hostage.

To mitigate the risk of ransomware attacks, users are strongly advised to set strong passwords that incorporate a variety of characters and to avoid connecting to unknown public networks. Connecting to such networks increases the chances of hackers gaining unauthorized access to devices. Additionally, organizations should consider requesting their IT department to

conduct educational sessions on ransomware attacks and cybersecurity for all employees These sessions should cover the dangers of ransomware, its propagation through phishing attacks, and its impact on data security within the organization(Tamburello, 2017). It is crucial to inform all employees about the risks associated with ransomware attacks, as the safety of the organization heavily relies on their responsible internet usage behavior.

4.2 Prevention of Clicking on Attachments or Links

Ransomware can be disseminated through various methods, with the most commonly known approach being phishing attacks. In this type of attack, the attacker crafts an email and deceives the victim into clicking on attachments or links that contain malicious code. These malicious contents can be sent in different forms, such as PDF, ZIP, Word Doc, or JavaScript(*.pdf,*.doc,*.cmd,*.exe,*.scr,*.jar files). Once the victim clicks on the attachments or links, they are redirected to a malicious website. The harmful file then infiltrates the victim's device without their knowledge, leading to actions such as device lock, file and program encryption, information theft, and more.

For employees within an organization, It is recommended to visit and access a safety site based on a "whitelist" approach. This approach allows specific programs to run on the devices while blocking any disallowed programs, thus preventing malicious attacks.

5. PREVENTION

The widespread use of science and technology, particularly the internet, has brought numerous benefits and improved the quality of life for humanity. This has been especially evident during the pandemic from 2020 to 2021, as people relied on technology to cope with the impact of Covid-19. For example, employees were able to work remotely through the internet, and students continued their education through online classes. However, along with the advantages, science and technology caused significant harm to society, such as cybercrime and cyber-attacks. Cyber attackers aim to steal and encrypt user's files in order to extort money using malicious software. To regain access to their files and devices, users are forced to pay a ransom demand using cryptocurrency like bitcoins. One of the most damaging cyber-attacks in recent years was the WannaCry ransomware attack in May 2017, which affected around 230,000 devices worldwide. This malware encrypts and holds the user's files, programs, or data hostage, and the only way to retrieve the encrypted files is by paying the ransom demand. However, there are various methods proposed by the authors to prevent ransomware infection, which will be discussed in this section.

5.1 Update Operating System and Security Software

Updating the operating system and security software is crucial to protect against potential attacks. Users who are unaware of the consequences of using outdated systems and software are at risk. Outdated operating systems and software lack the necessary defense mechanism and protection, making them vulnerable to attacks. Additionally, outdated operating systems may not support the latest updates released by vendors, further compromising their security. Attackers actively seek out security vulnerabilities and exploit them to target victims. Therefore, it is essential to ensure that the operating system, explorer, and defender applications are always up to date. Installing third-party plug-ins, such as Java and Flash Player, is strongly recommended to enhance devices safety, provided that the device supports them. However, it is important to note that while these measures can protect the devices to some extent, they do not guarantee complete immunity from harm.

5.2 User Awareness

The propagation of ransomware often begins with the presence of deceptive emails, links and attachments in the browser. The user's role in safeguarding their device, files and data from ransomware attacks is crucial, necessitating a constant awareness of cyber-related news. It is highly recommended that users actively participate in educational programs and research on malware attacks, as this is the prevailing trend. A fundamental practice for users to adopt is the establishment of robust passwords for all accounts on their devices, including software, email, and financial accounts. For instance, users should refrain from opening or viewing emails from unauthorized senders and should scan emails before reviewing them. If a suspicious file is detected, the email should be categorized as spam. Users must exercise caution when connecting to public networks. Consequently, the installation of paid software is always advisable for users, as it serves specific purposes. Many users opt to install cracked versions of paid software from free websites due to the high cost associated with some paid software. However, they fail to recognize that certain websites or download buttons for cracked software may contain malicious files that can compromise the security of their devices. Users must exercise prudence and carefully consider their actions before proceeding with any downloads.

In order to enhance employee awareness regarding network usage during work, the organization may consider conducting a talk or seminar. This initiative aims to mitigate the risk of ransomware attacks on the organization's system by ensuring that employees comprehend the potential consequences of such attacks. One valuable recommendation for employees is to refrain from logging into their email accounts and avoid browsing unfamiliar websites on their work machines. This precautionary measure is crucial because malicious attackers often employ tactics such as crafting deceptive emails containing intriguing subject lines, which may include malicious files. Consequently, if an employee falls prey to such a deceptive email, the harmful file will infiltrate and propagate throughout the machine.

5.3 Test Software on an Isolated PC or Operating System

Software that is downloaded from the whole site gets an opportunity containing the vindictive programming or document to introduce together in a gadget. Nobody of the clients can anticipate all the product downloaded is totally liberated from malware. To try not to introduce along with the noxious documents, the client can attempt to introduce the product in a detached PC that has not to associate with different gadgets and organizations. The disease won't spread to another gadget or organization in the event that product containing a ransomware document. Assuming the client understands that the product is introduced with the payment record, they can uninstall entire the working framework or reformat the gadget. This counteraction could decrease the pace of disease, saving time for recuperating the information in the gadget and stay away from monetary misfortunes.

CONCLUSION

This paper examines ransomware, including its history, forms, prevention strategies, and notable occurrences. There are many different types of ransomwares which can cause damage our data.Scareware, Encrypting ransomware, Screen lockers, Mobile ransomware, Doxware, DDoS extortion, Ransomware-as-a-Service(RaaS).

Regularly updating systems and software is also crucial. Understanding the different types of ransomwares is essential for effective prevention. We can prevent from ransomware by the techniques such as Update Operating System and Security Software, User Awareness, Test Software on an Isolated PC or Operating System and Prevention of Clicking on Attachments or Links.

In conclusion, the escalating threat of ransomware necessitates ongoing efforts to enhance cybersecurity measures and promote awareness. By implementing robust prevention techniques and remaining informed about evolving attack methods, both individuals and organizations can significantly reduce their susceptibility to ransomware threats.

ACKNOWLEDGEMENT

I would like to express my gratitude and appreciation to all those who gave me the possibility to complete this research paper and I am sincerely thankful to them for providing this opportunity to us.

I am also thankful to all the Faculty Members of Department of Research and PG studies in science & management, Vidyabharti Mahavidyalaya Camp Road, Amravati and Particularly my mentor Dr. S. R. Thakre for helping us during this research.

REFERENCES

1. Yan Lin Tiu & Mohammad Fadli Zolkipli(2021), Journal Of IT in Asia, volume-9, December 2021 https://www.researchgate.net/publication/357120305_Study_on_Prevention_and_Solution_of_Ransomware_Attack
2. https://www.proofpoint.com/us/threat-reference/ransomware
3. A. K. Maurya, N. Kumar, A. Agrawal, R. A. Khan(2018), Ransomware: Evolution, Target and Safety Measures, International Journal of Computer Sciences and Engineering ,volume-6 Issue-1, January 2018
4. J. Jones and N. Shashidhar, Ransomware Analysis and Defense WannaCry and the Win32 environment(, INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE ,Volume-6, No.4
5. Richardson R., North M. M. & Garofalo D.(2021), International Management Review, Ransomware: The Landscape Is Shifting --A Concise Report, Volume-17 No.,1